TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Mars 2021

#cyberväder berättar om betydande säkerhetsincidenter och -fenomen under månaden. Läsaren får en snabb helhetsbild av vad som hänt på cybersäkerhetsfältet under perioden i fråga. Läget kan vara:

lugnt

oroande

allvarligt

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder mars 2021

Dataintrång och dataläckor

- Exchange-situationen har stabiliserat och lugnat sig efter början av mars.
- Uppgifter som stals från Facebook år 2019 har offentliggjorts, bland dem finns även uppgifter om finländska användare.

Bluff och nätfiske

- Bluffmeddelanden med OmaPosti som tema är fortsättningsvis en daglig förtret.
- Bedrägerisamtal från falsk teknisk support plågar ännu finländarna – mest på engelska, men ibland även på dålig finska.

Skadeprogram och sårbarheter

- Det skadliga programmet BazarLoader sprids via e-post. Kampanjen är även känd under namnet BazarStrike.
- SMS med OmaPosti som tema leder i vissa fall också till skadeprogram.

Automation och IoT

- Ett stort dataintrång har gjorts mot bakgrundssystemen till nätverksprodukter från tillverkaren Ubiquiti.

Nätens funktion

- Fem stora funktionsstörningar.
- Upprepade funktionsstörningar i identifieringen av användare av riksomfattande digitala hälsotjänster.
- Att störa miljöer för distansundervisning med överlastningsangrepp är inte ett oskyldigt nöje, utan leder till brottsutredning.

Spionage

- Enligt Skyddspolisen låg en APT31-operation bakom dataintrånget mot riksdagen.
- Flera APT-grupper med koppling till Kina har under den senaste tiden varit aktiva på olika håll i världen.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Top 5 cyberhot - betydliga fenomen över en längre period

1 ↑

Sårbarheter som inte åtgärdas öppnar vägen för brottslingar till organisationen. Sårbarheter utnyttjas snabbt. Man lämnar enheter och tjänster öppna på nätet, utan att ha beaktat deras informationssäkerhet eller sett till att skyddsåtgärderna och underhållet är tillräckliga.

2 →

Användningen av olika typer av cyberangrepp för utpressning blir allt vanligare och hotar affärsverksamheternas kontinuitet. I Finland kommer det att ske allt fler webbattacker, där tiotusentals euro är småpengar.

3 ↓

Nätfiske
är mycket vanligt, och det kan vara svårt för mottagare av ett nätfiskemeddelande att observera bedrägeri. Detta utnyttjas även för riktade angrepp och spionage.

↑ *ökat*

↓ *minskat*

→ *oförändrat*

Gult = nytt/ uppdaterat*

4 →

Svag hantering av cyberrisker och oklar ansvarsfördelning för hantering av tjänster Det är svårt att förutspå konsekvenserna för cyberhot, och oklarheter vid ansvarsfördelningen för hantering av tjänster försämrar informationssäkerheten.

5 →

Bristfällig logginformation utgör en risk i många organisationer. På grund av bristfällig insamling, uppföljning och förvaring av logginformation kan man inte observera eller utreda it-incidenter.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret